

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 322 091 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.06.2003 Bulletin 2003/26

(51) Int Cl.7: H04L 29/06

(21) Application number: 02258074.0

(22) Date of filing: 22.11.2002

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 19.12.2001 JP 2001385869

(71) Applicant: CANON KABUSHIKI KAISHA
Tokyo (JP)

(72) Inventor: Arai, Shunji,
c/o Canon Kabushiki Kaisha
Tokyo (JP)

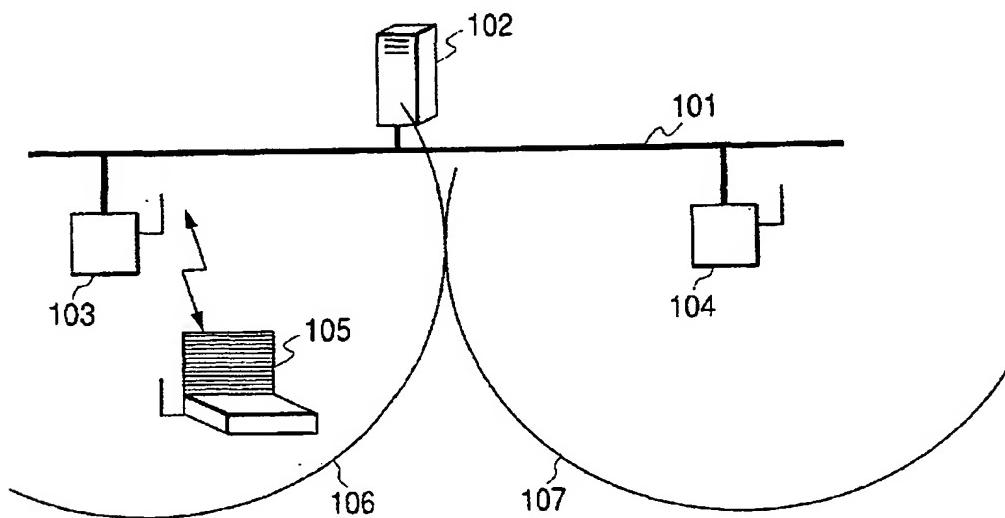
(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
2-5 Warwick Court,
High Holborn
London WC1R 5DH (GB)

(54) Communication system, server device, client device and method for controlling the same

(57) When a client server is permitted to be connected to a network through a first access point based on authentication by an authentication server, the authentication server informs the first access point of an encipher key such as a WEP key used for encipher communication between the client device and the first access point. Then, when the client device is moved to a com-

municable range of a second access point, the authentication server creates no new encipher keys but informs the second access point of the encipher key used for the encipher communication with the first access point, whereby encipher communication is executed between the client device and the second access point by using the same encipher key as that used for the encipher communication with the first access point.

FIG. 1



Description**BACKGROUND OF THE INVENTION****Field of the Invention**

[0001] The present invention relates to a communication system, in which a server device informs an access point of an encipher key used when a client terminal performs communication through the access point.

Description of the Related Art

[0002] Conventionally, in a wireless LAN system, a client terminal has been connected to a network through wireless communication with an access point on the network.

[0003] There is also a wireless LAN system, in which a client terminal receives authentication of connection to a network through an access point from an authentication server on a network.

[0004] In such a system, when the client terminal receives authentication from the authentication server, the client terminal and the authentication server create an encipher key of a wired equivalent privacy (WEP) encipher system, and the authentication server informs the access point of the created encipher key. Then, the client terminal transfers enciphered data with the access point by using the encipher key of the WEP encipher system to perform secure wireless communication.

[0005] Incidentally, a communicable range of the access point is limited to a range reached by electric waves. On the other hand, the client terminal can be freely moved. Accordingly, the client terminal may be moved from a communicable range of an access point 1 to a communicable range of an access point 2. In this case, the client terminal must receive authentication of connection to the network from the authentication server again through wireless communication with the access point 2, the client terminal and the authentication server must create a new WEP key, and the authentication server must inform the access point 2 of the new WEP key.

[0006] That is, when the client terminal changed the access point, re-authentication from the authentication server, creation of a new WEP key, informing of a WEP key, and the like prolonged the process until communication became possible. Consequently the process took time.

[0007] In addition, in a system of many client terminals, since authentication and creation of a WEP key prolonged a process, a load on an authentication server inevitably became large.

[0008] Furthermore, since the process took time when the access point was changed, usability was reduced.

SUMMARY OF THE INVENTION

[0009] A concern of the present invention is to improve usability of a system and a device.

[0010] Another concern of the present invention is to shorten time until communication becomes possible when a client terminal changes an access point.

[0011] Yet another concern of the present invention is to reduce a process when a client terminal changes an access point.

[0012] Other features of the present invention will become apparent upon reading of detailed description and drawings.

15 BRIEF DESCRIPTION OF THE DRAWINGS**[0013]**

20 FIG. 1 is a configuration view of a system according to an embodiment of the present invention.

FIG. 2 is a block diagram of an access point according to the embodiment of the invention.

FIG. 3 is a block diagram of a client terminal according to the embodiment of the invention.

FIG. 4 is a sequential view showing a system operation according to the embodiment of the invention.

FIG. 5 is a sequential view of the system operation according to the embodiment of the invention.

30 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] Next, description will be made of an embodiment of the present invention.

35 [0015] FIG. 1 is a configuration view of a system according to the embodiment of the invention.

[0016] A reference numeral 101 denotes a network, to which an access point A103, and an access point B104 are connected. The two access points are shown 40 in FIG. 1, but the number of installed points is not limited to two. Each of the access points A103 and B104 can perform wireless communication with a client terminal 105 present in communicable ranges 106, 107. According to the embodiment, as a wireless communication system, a wireless local area network (LAN) based on a standard such as IEEE 802.11, IEEE 802.11b, or IEEE 802.11a is used.

[0017] The reference numeral 105 is the client terminal, which is connected to the network 101 through wireless communication with the access point A103 or B104. Though not shown in FIG. 1, a plurality of client terminals 105 may be present.

[0018] A reference numeral 102 denotes an authentication server, which authenticates the client terminal 105 connected to the network 101; and creates an encipher key used in a wired equivalency privacy (WEP) encipher system.

[0019] FIG. 2 is a block diagram of the access point

A103.

[0020] A case of the access point B104 is similar.
 [0021] A reference numeral 201 denotes a wireless unit, which transfers wireless data. The wireless unit 201 is constituted of a transmission unit 210, a reception unit 211, and an antenna 212.

[0022] A reference numeral 202 denotes a signal process unit, which detects a signal received by the reception unit 211 to convert it into a digital signal, and modulates the signal in order to transmit a digital signal sent from a data process unit 203 by wireless. In addition, the signal process unit 202 has a function of adding a header or the like in order to use data sent from the data process unit 203 for wireless transmission, and removing a header or the like from received data to send it to the data process unit 203.

[0023] The reference numeral 203 is the data process unit, which is constituted of a transmission data process unit 205 for enciphering data from a network interface 208 by a WEP encipher system, and a reception data process unit 206 for decoding enciphered data.

[0024] A reference numeral 204 denotes a control unit, which executes determination of presence of a new client terminal 105, control of the entire access point A103, and the like.

[0025] A reference numeral 207 denotes a storage unit, which stores an encipher key for WEP enciphering, and information regarding an ID or the like of the client terminal 105.

[0026] The reference numeral 208 is the network interface, which is an interface between the access point A103 and the network 101.

[0027] FIG. 3 is a block diagram of the client terminal 105.

[0028] The client terminal 105 of the embodiment is constituted of a wireless communication card.

[0029] Functions similar to those of the access point A103 shown in FIG. 2 are denoted by similar numerals.

[0030] A reference numeral 301 denotes a data communication interface, which is connected to an information processor such as a personal computer to perform data communication.

[0031] A reference numeral 302 denotes a storage unit, which stores an encipher key for WEP enciphering, and information regarding an ID or the like of the client terminal 105 necessary for wireless communication with the access point A103 or the access point B104. According to the embodiment, as an ID of the client terminal 105, a media access control (MAC) address is used.

[0032] Next, description will be made an operation of the entire system of the embodiment with reference to the drawings.

[0033] First, a process of first connection of the client terminal 105 to the network 101 through the access point A103 is explained by referring to a sequential view of FIG. 4.

[0034] The client terminal 105 executes open authentication in the wireless LAN to be connected to the ac-

cess point A103 (S401).

[0035] The access point A103 obtains an ID of the client terminal 105 (S402).

[0036] The access point A103 informs the authentication server 102 of the ID of the client terminal 105 (S403).

[0037] The authentication server 102 determines whether authentication for the connection of the client terminal 105 to the network 101 has been finished or not, based on the ID informed from the access point A103 (S404). The client terminal 105 makes the connection for the first time, and the authentication has not been finished. Thus, it is determined that the authentication has not been finished.

[0038] The authentication server 102 requests the client terminal 105 to input a user name and a password (S405).

[0039] The client terminal 105 inputs the user name and the password (S406).

[0040] In order to enhance secrecy of the user name and the password inputted in step S406, the client terminal 105 executes irreversible numerical value processing called one-way hash, and informs the authentication server 102 of its one-way hash data (S407).

[0041] The authentication server 102 collates the one-way hash data informed in step S407 with a data group regarding a user for permitting connection to the network 101, which is saved in a database in the authentication server 102. If a result of the collation shows coincident data, the connection to the network 101 is permitted to the client terminal 105, and the ID of the client terminal 105 is stored (step S408).

[0042] The client terminal 105 and the authentication server 102 create an encipher key called a WEP session key (S409). The WEP session key is an encipher key, which is used in the WEP encipher system, and valid only for enciphering traffic of the client terminal 105.

[0043] The authentication server 102 stores the created WEP session key in association with the ID of the client terminal 105, and informs it to the access point A103 (S410).

[0044] The access point A103 enciphers a broadcast key with the WEP session key (S411), and sends the enciphered broadcast key to the client terminal 105 (S412). The broadcast key is an encipher key, which is used when data broadcast from the access point A103 to a plurality of client terminals 105 is enciphered.

[0045] The client terminal 105 decodes the enciphered broadcast key by using the WEP session key created in step S409 to obtain a broadcast key (S413).

[0046] The access point A103 and the client terminal 105 start WEP encipher sequences (S414, S415).

[0047] Then, in communication with one client terminal 105 (point-to-point communication, the access point A103 transfers data enciphered with the WEP session key to perform secure wireless communication (S416). In broadcast communication with a plurality of client terminals 105 (point-to-multipoint communication), the ac-

cess point A103 transfers data enciphered with the broadcast key to perform secure wireless communication (S416).

[0048] Fig. 5 shows a sequential view of an operation when the client terminal 105, for which authentication of its connection to the network 101 through the access point A103 has been finished, is moved from the communicable range 106 of the access point A103 to the communicable range 107 of the access point B104 to be connected to the network 101 through the access point B104.

[0049] The client terminal 105 is moved out of the communicable range 106 of the access point A103 to be incommunicable with the access point A103 (S501). Then, the client terminal 105 is moved into the communicable range 107 of the access point B104 to be communicable with the access point B104.

[0050] The client terminal 105 executes open authentication to be connected to the access point B104 (S502).

[0051] The access point B104 obtains an ID of the client terminal 105 (S503).

[0052] The access point B104 informs the authentication server 102 of the ID of the client terminal 105 (S504).

[0053] The authentication server 102 determines whether authentication for the connection of the client terminal 105 to the network 101 has been finished or not, based on the ID informed in step S504, and the stored ID of the client terminal 105, for which the authentication has been finished (S505). Here, for the client terminal 105, the authentication of its connection to the network 101 through the access point A103 was finished in step S408 (FIG. 4), and the ID of the client terminal has been stored. Thus, it is determined that the authentication has been finished.

[0054] The authentication server 102 instructs the access point A103 to delete the WEP session key stored in the storage unit 207 to be used for wireless communication with the client terminal 105 (S506).

[0055] The authentication sever 102 informs the access point B104 of the WEP session key stored in association with the ID of the client terminal 105 in step S410 (FIG. 4) (S507).

[0056] The access point B104 enciphers a broadcast key with the WEP session key informed in step S507 (S508), and sends the enciphered broadcast key to the client terminal 105 (S509).

[0057] The client terminal 105 decodes the enciphered broadcast key by the WEP session key created in step S409 (FIG. 4) to obtain a broadcast key (S510).

[0058] The access point B104 and the client terminal 105 start WEP encipher sequences (S511, S512).

[0059] Then, in communication with one client terminal 105 (point-to-point communication), the access point B104 transfers data enciphered with the same WEP session key as that used for the communication between the client terminal 105 and the access point

A103 to perform secure wireless communication (S513). In broadcast communication with a plurality of client terminals 105 (point-to-multipoint communication), the access point B104 transfers data enciphered with the broadcast key to perform secure wireless communication (S513).

[0060] In the embodiment, in step S507, the WEP session key stored in the authentication server 102 is informed to the access point B104. However, the WEP session key stored in the access point A103 may be informed through the authentication server 102 to the access point B104.

[0061] In the foregoing explanation, the client terminal 105 was the wireless communication card. However, a function similar to the wireless communication card may be incorporated in a personal computer or personal digital assistants (PDA).

[0062] Needless to say, the object of the present invention can be achieved by supplying a storage medium, in which software program codes for realizing the functions of the client terminal, the access points, and the authentication server are stored, to a system or a device, and causing the system or a computer (alternatively CPU or MPU) of the device to read and execute the program codes stored in the storage medium.

[0063] In such a case, the program codes read from the storage medium realize the functions of the embodiment themselves, and the storage medium, in which the program codes are stored, constitutes the present invention.

[0064] As the storage medium for supplying the program codes, a ROM, a floppy disk, a hard disk, an optical disk, a magneto-optical disk, a CD-ROM, a CD-R, a magnetic tape, a nonvolatile memory card or the like can be used.

[0065] Needless to say, not only the case of realizing the functions of the embodiment by executing the program codes read by the computer, but also a case where based on instructions of the program codes, a part or all of the actual process is executed by an OS or the like working on the computer to realize the functions of the embodiment are included in the present invention.

[0066] Furthermore, needless to say, a case where the program codes read from the storage medium are written in a CPU or the like provided in a function extension board inserted into the computer or a function extension unit connected to the computer and, then, based on instructions of the program codes, the CPU or the like provided in the function extension board or the function extension unit executes a part or all of the actual process to realize the functions of the embodiment is included in the present invention.

[0067] As described above, according to the present invention, it is possible to enhance usability of the device.

[0068] It is possible to shorten time until communication becomes possible when the client terminal changes an access point.

[0069] Moreover, it is possible to reduce a process when the client terminal changes an access point.

Claims

1. A communication system comprising:

creation means for creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and informing means for informing the first access point of the encipher key created by the creation means,

wherein the informing means informs a second access point of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

2. A server device comprising:

creation means for creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and informing means for informing the first access point of the encipher key created by the creation means,

wherein the informing means informs a second access point of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

3. The server device according to claim 2, further comprising: instruction means for instructing the first access point to delete the encipher key when the client terminal is connected to the network through the second access point.

4. The server device according to claim 2, wherein the encipher key which the informing means informs to the second access point is an encipher key stored when the encipher key is created by the creation means, or an encipher key received from the first access point.

5. A server device for informing an access point of an encipher key used when a client terminal performs communication through the access point, comprising:

5

determination means for determining transition of the client terminal from communication through a first access point to communication through a second access point; and informing means for informing the second access point of the same encipher key as that informed to the first access point based on the determination of the determination means.

10 6. A server device comprising:

authentication means for authenticating connection of a client device to a network through an access point; informing means for informing an access point, to which the client device is connected, of an encipher key in accordance with a result of the authentication by the authentication means; and

determination means for determining whether the client device which requests the authentication means to execute authentication is a client device or not, for which authentication has been finished,

wherein the informing means informs the access point, to which the client device is connected, of a new encipher key in accordance with the determination of the determination means.

25 7. The server device according to claim 6, wherein the informing means informs the access point, to which the client device is connected, of a new encipher key if the determination means determines that the client device which requests the authentication has been unauthenticated, and the access point, to which the client device is currently connected, of the same encipher key as that informed to an access point in previous authentication if it is determined that the client device is the client device, for which the authentication has been finished.

30 8. A client terminal connected to a network through an access point, comprising:

creation means for creating an encipher key used for communication with a first access point; and communication means for executing encipher communication with the first access point by using the encipher key created by the creation means,

wherein the communication means uses the encipher key used for the encipher communication with the first access point even when an access point connected for connection to the network is changed from the first access point to a second ac-

cess point.

9. The client terminal according to claim 8, further comprising: receiving means for receiving a permission notice of the connection to the network from an authentication server,

wherein the creation means creates the encipher key in accordance with the reception of the permission notice by the receiving means.

10. A control method for a communication system, comprising the steps of:

creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and

informing the first access point of the encipher key created by the creation means,

wherein in the informing step, a second access point is informed of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

11. A control method for a server device, comprising the steps of:

creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and

informing the first access point of the encipher key created by the creation means,

wherein in the informing step, a second access point is informed of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

12. A control method of a server device for informing an access point of an encipher key used when a client terminal performs communication through the access point, comprising the steps of:

determining transition of the client terminal from communication through a first access point to communication through a second access point; and

informing the second access point of the same encipher key as that informed to the first access point based on the determination of the determination step.

5

13. A control method for a server device, comprising the steps of:

authenticating connection of a client device to a network through an access point; informing an access point, to which the client device is connected, of an encipher key in accordance with a result of the authentication in the authentication step; and determining whether the client device which requests authentication in the authentication step is a client device or not, for which authentication has been finished;

10

wherein in the informing step, the access point, to which the client device is connected, is informed of a new encipher key in accordance with the determination in the determination step.

15

14. A control method for a client terminal connected to a network through an access point, comprising the steps of:

creating an encipher key used for communication with a first access point; and executing encipher communication with the first access point by using the encipher key created in the creation step,

20

wherein in the communication step, the encipher key used for the encipher communication with the first access point is used even when an access point connected for connection to the network is changed from the first access point to a second access point.

25

30

35

40

45

50

55

FIG. 1

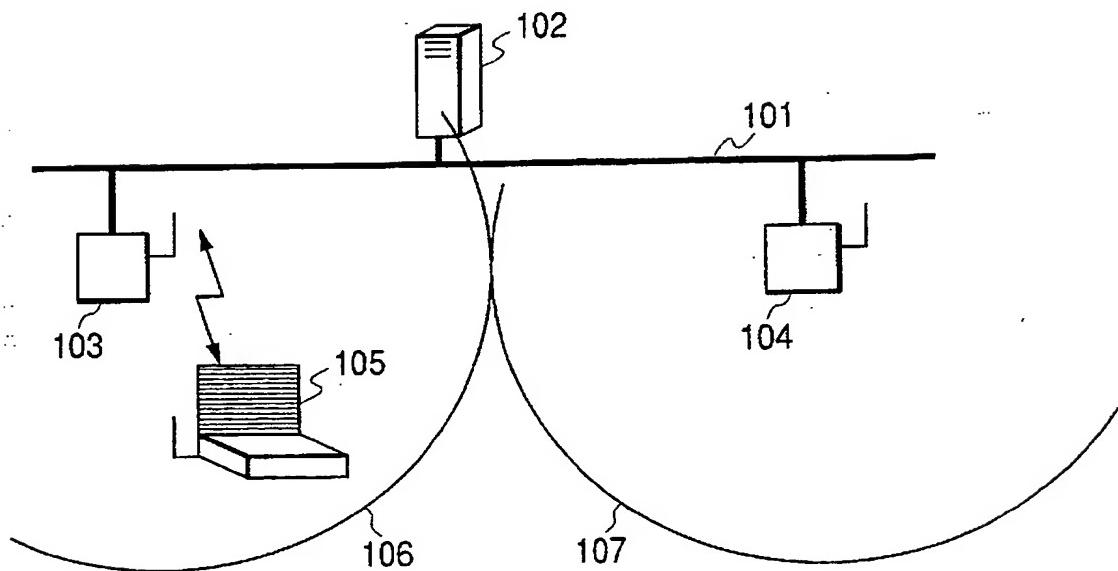


FIG. 2

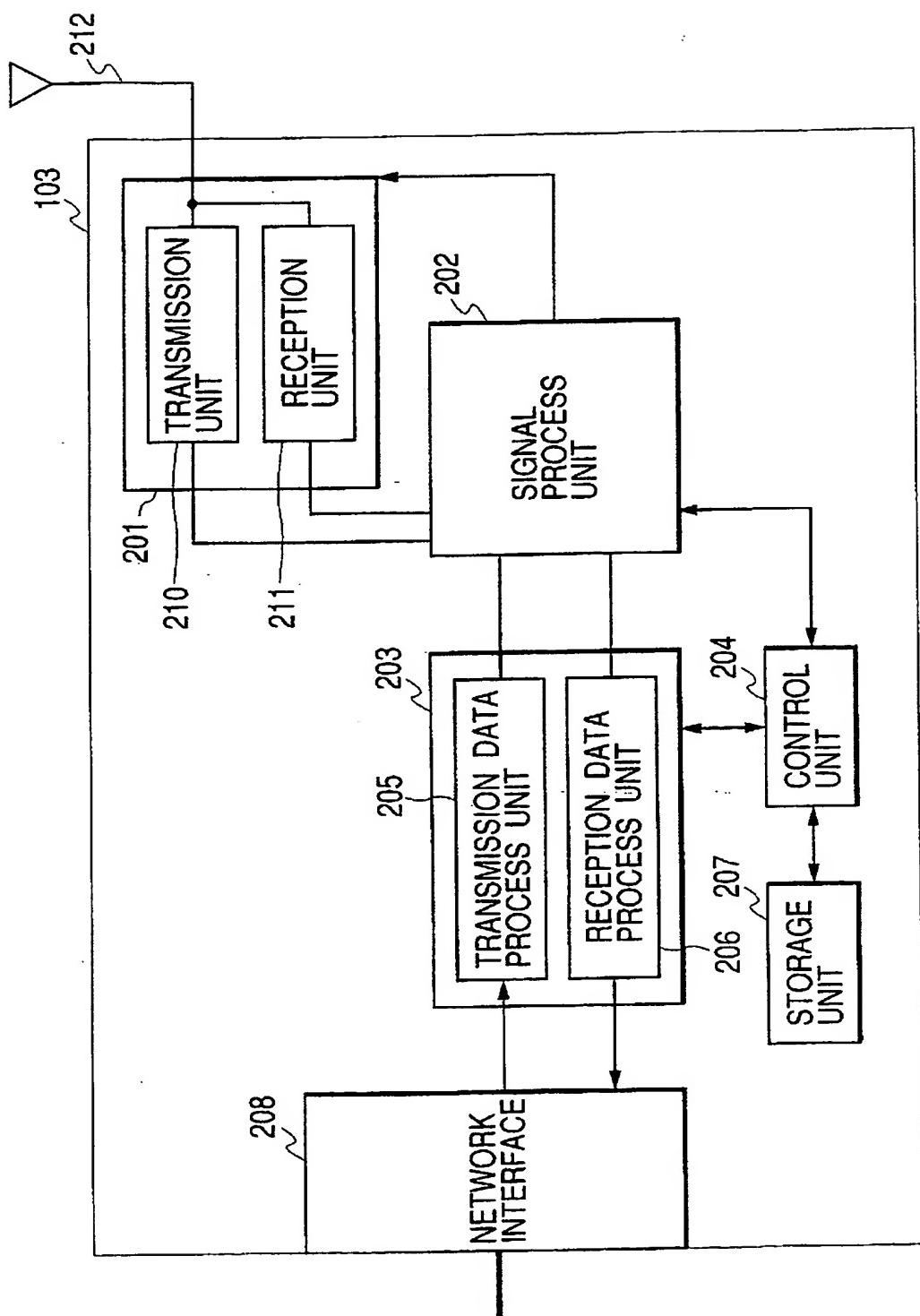


FIG. 3

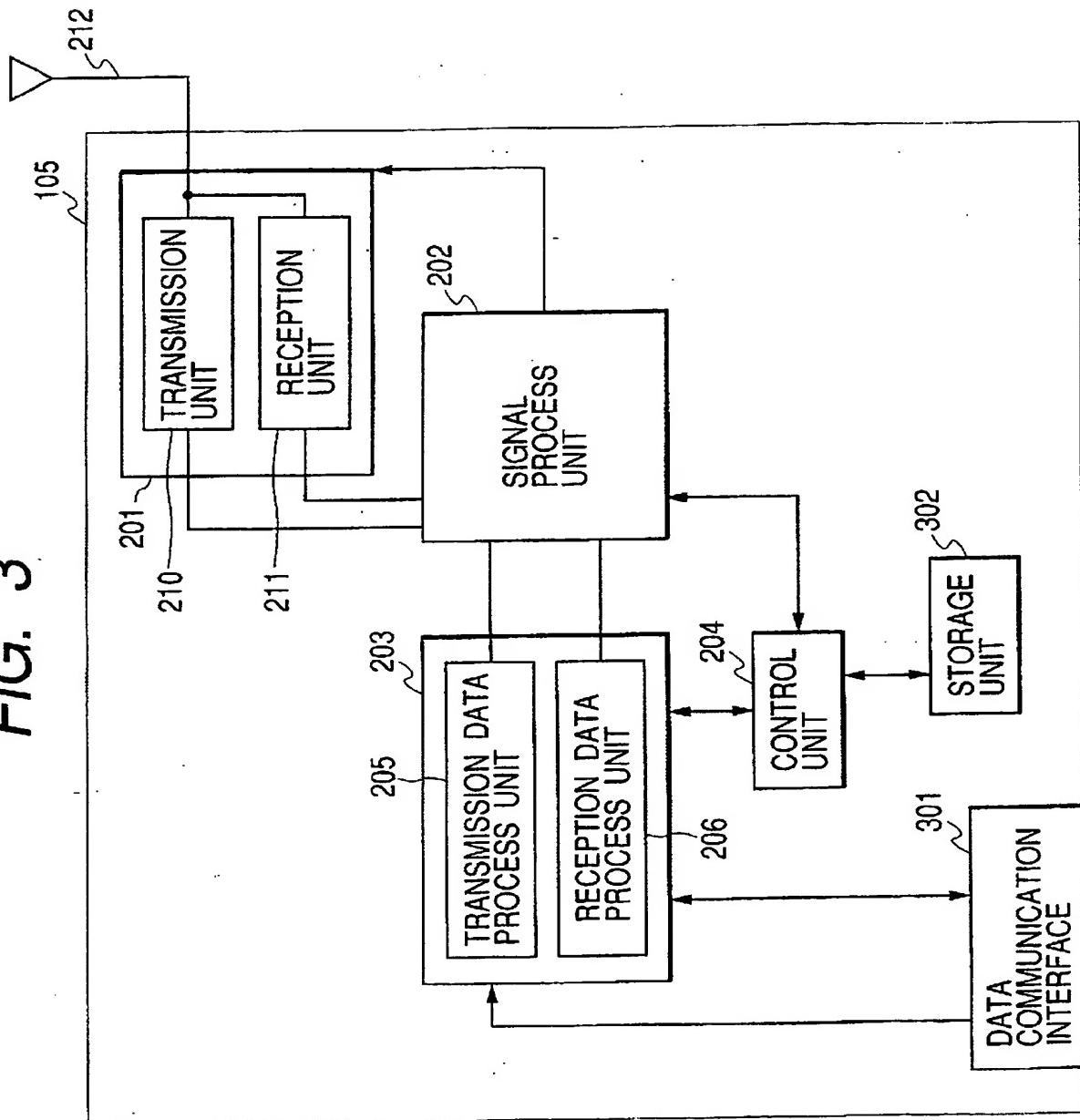


FIG. 4

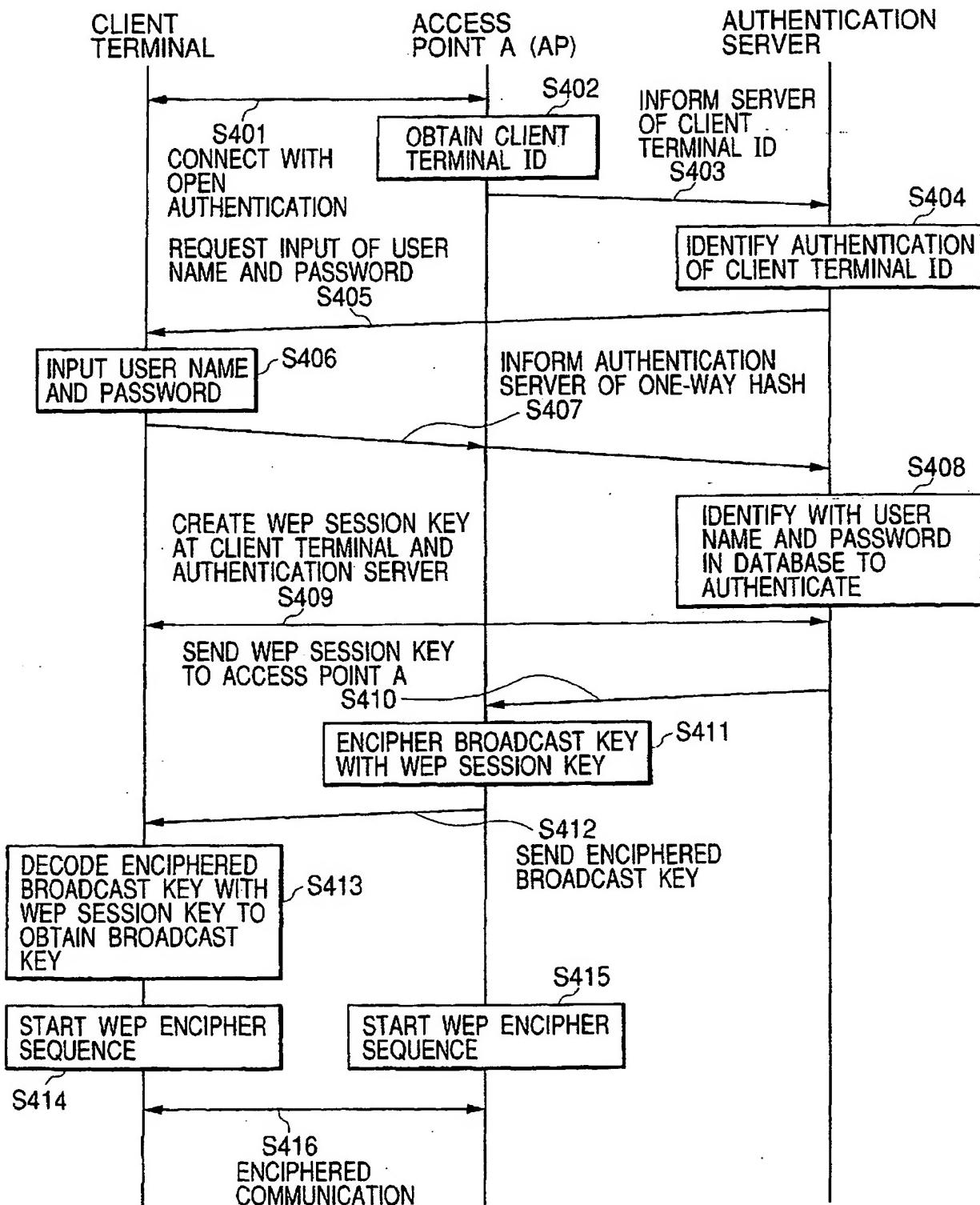
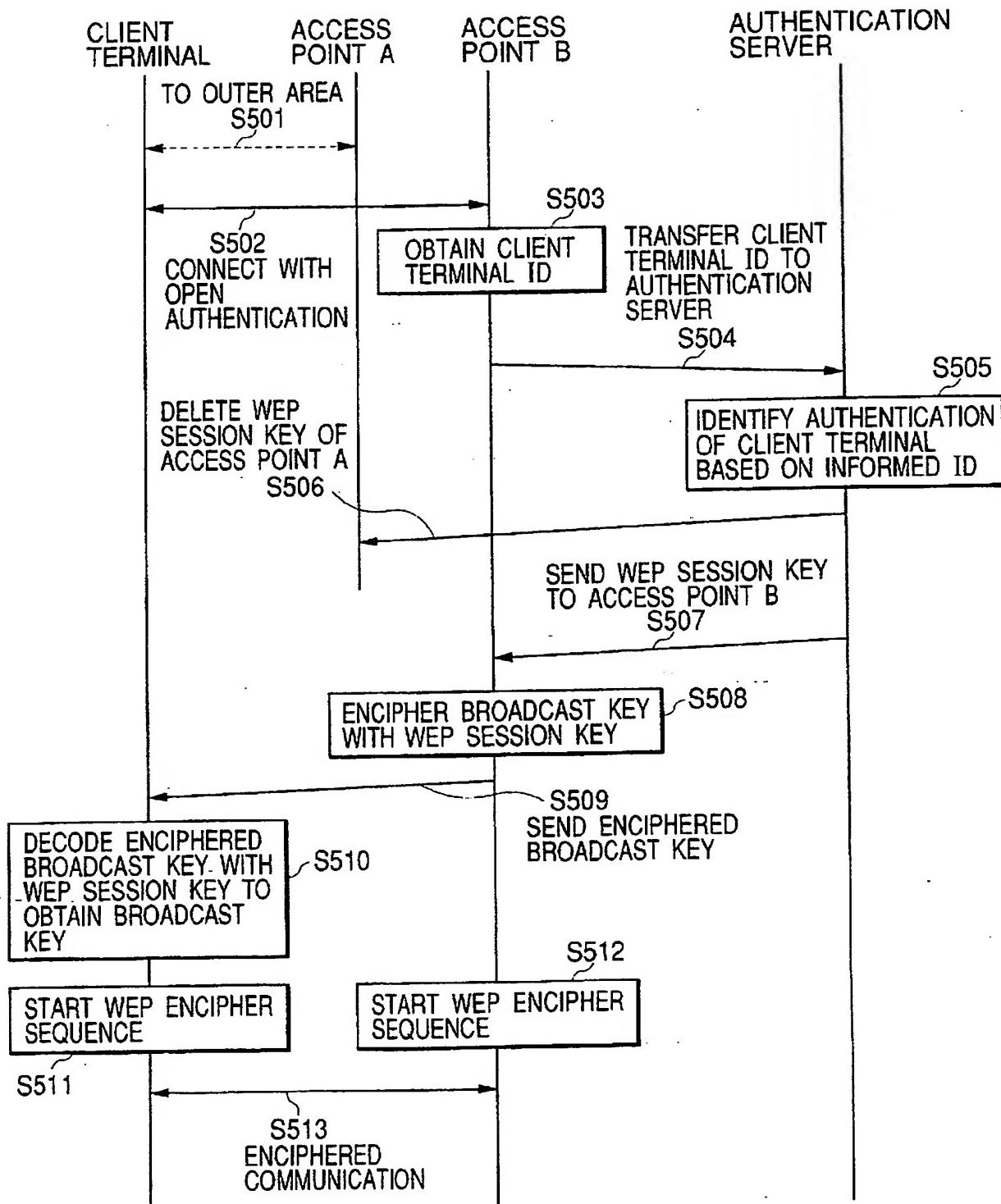


FIG. 5





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 25 8074

DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int.Cl.7)			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	H04L29/06			
P,X	WO 02 096151 A (FLARION TECHNOLOGIES INC ;VANDERVEEN MICHAELA CATALINA (US)) 28 November 2002 (2002-11-28) * abstract * * page 9, line 19 - line 20 * * page 11, line 21 - line 26 * * page 13, line 5 - line 8 * * page 13, line 24 - page 14, line 6 * * page 14, line 21 - line 28 * * page 15, line 7 - line 19 * * page 19, line 5 - line 23 * * figures 2-7 * ---	1,8-10, 14	H04L29/06			
X	WO 01 24560 A (SIMOCO INT LTD ;RAYNE MARK WENTWORTH (GB)) 5 April 2001 (2001-04-05) * page 7, line 28 - page 8, line 8 * ---	8,9,14				
A	WO 01 22685 A (ERICSSON TELEFON AB L M) 29 March 2001 (2001-03-29) * page 2, line 32 - page 4, line 15 * * page 4, line 14 - page 5, line 32 * * page 7, line 21 - page 8, line 16 * * page 11, line 1 - page 13, line 27 * ---	1-14	TECHNICAL FIELDS SEARCHED (Int.Cl.7)			
A	T. TANAKA,M.MORIKURA,H.TAKANASHI: "Nomadic Computing Environment Employing Wired and Wireless Networks" IEICE TRANS. COMMUN., vol. E81-B, no. 8, 12 January 1998 (1998-01-12), XP000788462 * page 1569, right-hand column, line 14 - page 1571, right-hand column, line 47 * -----	1-14	H04L H04Q			
The present search report has been drawn up for all claims						
Place of search	Date of completion of the search	Examiner				
THE HAGUE	23 April 2003	Olaechea, F				
CATEGORY OF CITED DOCUMENTS						
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document						
T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document						

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 02 25 8074

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
 The members are as contained in the European Patent Office EDP file on
 The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

23-04-2003

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
WO 02096151	A	28-11-2002	WO US	02096151 A1 2002197979 A1	28-11-2002 26-12-2002
WO 0124560	A	05-04-2001	AU WO GB	7534900 A 0124560 A1 2359464 A	30-04-2001 05-04-2001 22-08-2001
WO 0122685	A	29-03-2001	SE AU WO SE	519471 C2 7694200 A 0122685 A1 9903370 A	04-03-2003 24-04-2001 29-03-2001 21-03-2001



Application No: GB0418886.8

Examiner: Steve Evans

Claims searched: All

Date of search: 16 February 2005

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	-	EP 1322091 A (CANON) - Whole document

Categories:

X Document indicating lack of novelty or inventive step	A Document indicating technological background and/or state of the art
Y Document indicating lack of inventive step if combined with one or more other documents of same category.	P Document published on or after the declared priority date but before the filing date of this invention
& Member of the same patent family	E Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^X :

H4L

Worldwide search of patent documents classified in the following areas of the IPC⁰⁷

H04L; H04Q

The following online and other databases have been used in the preparation of this search report

Online: WPI, EPODOC